Cybersecurity actions and protocols for the "Poder Judicial de Buenos Aires – Argentina"

Tomás Capelli[1][0009-0005-3878-7181], Alejandra Lliteras[1][0000-0002-4148-1299], Patricia Bazán[2][0000-0001-6720-345X]

[1] UNLP Facultad de Informática, LIFIA
[2] LINTI. Facultad de Informática, UNLP

Abstract. This paper explores cybersecurity issues in the technological infrastructure of the Suprema Corte de Justicia de Buenos Aires (SCBA) and proposes actions by and for the staff of the *Seguridad y Auditoria* Area (SyA). The increasing importance of cybersecurity in the SCBA is highlighted due to the digitization of files, electronic notifications, and remote access.
The technological infrastructure of the SCBA experienced a security event at the onset of the COVID19 pandemic, requiring rapid response and forcing the implementation of preventive security strategies, such as enhanced monitoring, reinforcement of security policies, deployment of advanced tools, and the development of a Com-prehensive Information Security Plan.
Approved in 2021, this Plan establishes security objectives including risk identification and analysis, the development of a regulatory framework, the creation and implementation of security protocols, ensuring regulatory compliance, and the cross-sectional application of security policy.
The goal of this paper is to identify cybersecurity-related problems within the technological infrastructure of the SCBA, to propose actions to be carried out by SyA and other Areas of the *Subsecretaría de Tecnología Informática* (STI) of the SCBA. These actions are intended to have a cross-cutting effect across all Areas that comprise the STI and its *Delegaciones de Tecnología Informática* (DTI).
The actions taken to guarantee an optimal level of cybersecurity in the technological infrastructure of the SCBA, as well as the implemented policies, are detailed.

Keywords: Cybersecurity, Integral Security Plan, Technological Asset.

Acciones y protocolos en ciberseguridad para el Poder Judicial de la Provincia de Buenos Aires - Argentina

Resumen. Este trabajo explora las problemáticas de ciberseguridad en la infraestructura tecnológica de la Suprema Corte de Justicia de Buenos Aires (SCBA) y propone acciones por parte y para el personal del Área de Seguridad y Auditoría

(SyA). Se destaca la creciente importancia de la ciberseguridad en la SCBA debido a la digitalización de expedientes, notificaciones electrónicas y acceso remoto.
La infraestructura tecnológica de la SCBA sufrió un evento de seguridad cuando comenzó la pandemia COVID19 debiendo dar respuesta rápidamente y obligando a encontrar estrategias de seguridad preventiva, como el mayor monitoreo, el fortalecimiento de políticas de seguridad, el despliegue de herramientas avanzadas y el desarrollo de un Plan Integral de Seguridad de la Información.
Dicho Plan, aprobado en 2021, establece objetivos de seguridad como la identificación y análisis de riesgos, la elaboración de un marco normativo, el desarrollo e implementación de protocolos de seguridad, el aseguramiento del cumplimiento normativo y la aplicación transversal de la política de seguridad.
Este trabajo tiene como objetivo identificar problemáticas relacionadas a ciberseguridad de la infraestructura tecnológica de la SCBA con el fin de proponer acciones a ser llevadas por parte SyA y de otras Áreas de la Subsecretaría de Tecnología Informática de la SCBA las cuales van a un efecto transversal a todas las Áreas que componen a la Subsecretaría y a sus Delegaciones de Tecnología Informática.
Se detallan las acciones llevadas a cabo para garantizar un nivel óptimo de ciberseguridad de la infraestructura tecnológica de la SCBA, así como las políticas implementadas.

Palabras clave: Ciberseguridad, Plan Integral de Seguridad, Activos Tecnológicos.

1 Introducción

La Suprema Corte de Justicia de Buenos Aires (SCBA)[1] es el máximo órgano del Poder Judicial de dicha provincia. El Poder Judicial de Buenos Aires se compone de veinte departamentos judiciales, los cuales cada uno se encuentran compuestos por una cabecera y distintos juzgados de paz. Existen localidades que no cuentan con un organismo de cabecera, pero sí con un juzgado de paz, como, por ejemplo: San Carlos de Bolívar que pertenece al departamento judicial Azul.

A su vez, la Suprema Corte de Justicia cuenta con organismos de administración de justicia como pueden ser la Secretaría de Administración, Secretaría de Personal, Subsecretaría de Control Disciplinario, Dirección General de Asesorías Periciales, entre otras.

Por otro lado, la Suprema Corte de Justicia cuenta con la Subsecretaría de Tecnología Informática que es la encargada de "la dirección, coordinación y ejecución de los procesos de desarrollo, implantación y actualización de tecnologías de la información y comunicación en todo el ámbito de la Administración de Justicia"[2].

La infraestructura de tecnología de la Suprema Corte de Justicia se compone de un centro de datos propio, más de 19.000 puestos de trabajo, alrededor de 1.000 servidores y más de 30 aplicaciones críticas.

[1] www.scba.gov.ar
[2] https://www.scba.gov.ar/paginas.asp?id=39716

Cada uno de los veinte departamentos judiciales cuenta con una Delegación de Tecnología Informática la cual es responsable de los activos dentro de ella y responde al Área de Atención y Capacitación de Usuarios (previamente mencionada).

En el contexto previamente planteado, la ciberseguridad[3] ha adquirido una importancia fundamental dentro del Poder Judicial de la Provincia de Buenos Aires, especialmente debido a la creciente dependencia de los sistemas informáticos para la gestión de expedientes, notificaciones electrónicas y acceso remoto. La protección de estos sistemas no solo garantiza la continuidad operativa del servicio de justicia, sino que también preserva la confidencialidad, integridad y disponibilidad de la información procesada. En este marco, la implementación de estrategias de seguridad informática resulta clave para mitigar riesgos, prevenir ataques y fortalecer la infraestructura tecnológica de la Suprema Corte de Justicia.

Este trabajo tiene como objetivo identificar problemáticas relacionadas a ciberseguridad de la infraestructura tecnológica de la SCBA con el fin de proponer acciones a ser llevadas por parte del personal de la Subsecretaría de Tecnología Informática de la Suprema Corte de Justicia de la Provincia de Buenos Aires, ya sea el Área de Seguridad y Auditoría o el Área que tenga la responsabilidad sobre los activos, las cuales van a tener un efecto transversal a todas las Áreas que componen a la Subsecretaría y a sus DTI.

El documento se organiza de la siguiente manera: en la Sección 2 se describe un marco conceptual en torno a ciberseguridad y algunos aspectos normativos. La Sección 3 detalla la situación actual del organismo, para brindar una enumeración de las acciones llevadas a cabo, presentadas en la Sección 4. Finalmente, en la Sección 5 se enuncian las conclusiones y trabajos futuros.

2 Marco Conceptual y Contexto

La International Telecommunication Union (2009) señala que la ciberseguridad es: "*La colección de herramientas, políticas, conceptos de seguridad, salvaguardas, directrices, enfoques de gestión de riesgos, acciones, formación, mejores prácticas, garantías y tecnologías que pueden ser utilizadas para proteger el entorno cibernético y los activos del usuario*".

Pero el concepto no resulta nuevo, de hecho, según (Warner, M., 2012) el concepto de ciberseguridad comenzó a desarrollarse en la década de 1960, aunque no fue hasta los años 90 cuando tomó mayor relevancia dentro de las políticas gubernamentales. En esa época, el gobierno de los Estados Unidos identificó dos aspectos fundamentales que impulsaron la consolidación de esta disciplina: 1- la constatación de que las computadoras podían ser atacadas y sus datos robados; y 2- el reconocimiento de que estas vulnerabilidades podían ser explotadas con fines militares.

Ahora bien, resulta importante analizar su evolución y desarrollo a lo largo de los últimos veinte años. Para ello, se tomará como referencia el estudio presentado por

[3] "Es la práctica de proteger su información digital, dispositivos y activos." Fuente: https://url-shortener.me/YZR

(Furstenau et al., 2020) donde se proporciona un análisis detallado de los principales avances en la disciplina. En particular, en dicho estudio se examina el período abarcado entre 1999 y 2019, identificando los hitos y transformaciones claves que han marcado el desarrollo de la ciberseguridad. Una síntesis de lo anterior se presenta en la Fig. 1, donde es posible visualizar los distintos períodos y los acontecimientos que han definido la evolución del campo, permitiendo una comprensión más profunda de su consolidación como disciplina estratégica en el ámbito tecnológico y organizacional.

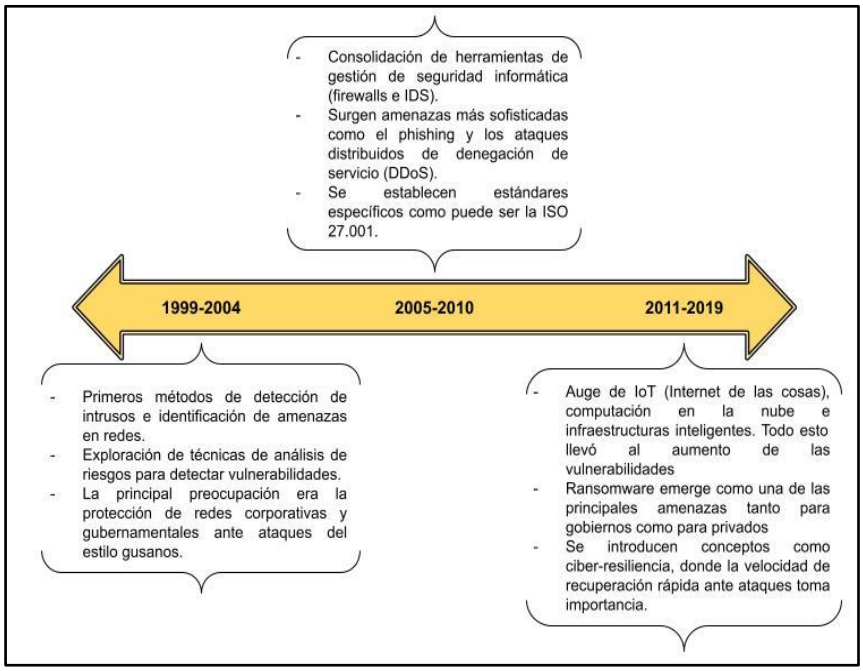

Fig 1. Acontecimientos en cada periodo de tiempo. Fuente: Elaboración propia a partir de (Furstenau, et al. 2020)

Asimismo, en el estudio de (Fustenau et al., 2020) se evidencia el creciente desarrollo de la ciberseguridad en el ambiente científico. Tal como se ilustra en la Fig. 2, se observa un incremento en la cantidad de publicaciones dedicadas a esta disciplina, reflejando su consolidación como un campo de estudio.

Para comprender con mayor profundidad los fundamentos de la ciberseguridad y su relevancia en el contexto actual, resulta imprescindible definir algunos conceptos clave que constituyen la base de esta disciplina. En este sentido, el eje central de toda actividad orientada a la protección de la información se encuentra atravesada por la conocida tríada de la seguridad de la información, conformada por la Confidencialidad, la Integridad y la Disponibilidad (CIA). Estos tres principios, conocidos y estandarizados a nivel internacional, garantizan un enfoque integral en la gestión de la seguridad de los activos de información.

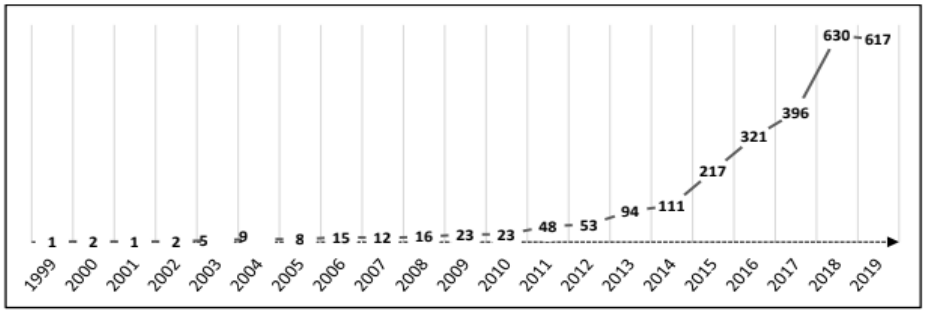

Fig. 2. Cantidad de publicaciones entre 1999 y 2019. Fuente: (Furstenau et al., 2020)

2.1 Definiciones

La ISO/IEC 27001:2022, define: 1- Confidencialidad, propiedad que garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella, 2- Integridad, capacidad para salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento, asegurando que los datos no sean alterados de manera indebida y 3- Disponibilidad, propiedad que garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera, permitiendo la continuidad operativa de los sistemas de información.

A esta tríada, se pueden sumar los conceptos de autenticidad y trazabilidad. Según MAGERIT 3.0 (Ministerio de Hacienda y Administraciones Públicas, 2012) El primer concepto, indica la propiedad de una entidad de ser quien dice ser o bien garantiza la fuente de la que proceden los datos. El segundo, refiere al aseguramiento de que en todo momento se puede determinar quién hizo qué.

Según el Plan Integral de Ciberseguridad de la Provincia de Buenos Aires (Gobierno de la Provincia de Buenos Aires, 2021), un activo es “todo aquello que genere, procese, almacene y transmita información, que tenga valor para una organización, y por lo tanto deba protegerse, incluido, pero no limitado a: hardware, software, información almacenada en cualquier tipo de medio, personas, reputación e imagen, entre otros”.

Si bien todos los activos poseen un valor inherente, algunos resultan especialmente críticos debido a su rol en el funcionamiento de las infraestructuras. En este sentido, la misma fuente define la infraestructura crítica como “aquella que resulta indispensable para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente”. La protección de estos elementos resulta fundamental dentro de cualquier estrategia de ciberseguridad, dado que su vulnerabilidad puede comprometer el desarrollo y la estabilidad de los servicios ofrecidos por el organismo.

Según MAGERIT 3.0 (Ministerio de Hacienda y Administraciones Públicas, 2012), una vulnerabilidad se define como un “defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza” y un riesgo es “la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización”.

La correcta evaluación y gestión del riesgo es fundamental para la implementación de estrategias de mitigación y control dentro de un sistema de seguridad de la información.

2.2 Antecedentes normativos

Desde el año 2019, la República Argentina cuenta con una normativa específica, actualizada en 2023 bajo el identificador RESOL-2023-44-APN-SIP#JGM[4], que aborda la problemática de la ciberseguridad a nivel federal. Esta disposición busca impulsar políticas públicas encaminadas a promover la creación de instancias institucionales en los ámbitos ejecutivo, legislativo y judicial de las provincias, fomentando la armonización y colaboración entre jurisdicciones para fortalecer la protección de la información.

La provincia de Buenos Aires, al igual que el Estado Nacional, ha desarrollado su propio marco normativo en materia de ciberseguridad, el cual fue aprobado y publicado en el año 2021 bajo la identificación Decreto 8/2021[5]. Esta normativa establece los lineamientos estratégicos para la protección de los activos digitales provinciales y la gestión integral de la seguridad de la información en el ámbito público.

El Plan Integral de Seguridad de la Información de la Suprema Corte de Justicia de Buenos Aires, establecido mediante la Resolución N.º 1649 del año 2021[6]. Este instrumento normativo se diseñó con el propósito de fortalecer la seguridad de los activos de información y, para ello, se consideró esencial alinear su desarrollo e implementación con las reglamentaciones vigentes del Gobierno de la Provincia de Buenos Aires, particularmente con lo estipulado en el Decreto 8/21.

Si bien el Poder Judicial posee autonomía en la adopción de disposiciones provinciales, en conformidad con la división de poderes del Estado, se determinó que la coordinación con las normativas provinciales era una estrategia fundamental para robustecer la protección de la información generada de manera continua a través de los diversos servicios que se prestan a la ciudadanía. Este enfoque permitió establecer mecanismos de seguridad alineados con los estándares provinciales y garantizando un nivel de protección adecuado para los datos judiciales.

Las normativas jurisdiccionales mencionadas - Nacional, Provincial y Judicial - presentan perspectivas únicas y desarrollos particulares en materia de seguridad de la información, pero presentan puntos en común: 1- adoptan una visión estratégica de la seguridad de la información, 2- resaltan la gestión efectiva del riesgo, 3- define un plan de continuidad y 4- realizan una adecuada gobernanza de los activos de información.

Además, las tres normativas destacan la necesidad de contar con programas de formación y concientización dirigidos a los usuarios, la detección y posterior protección de infraestructuras críticas, y la adopción de estándares y normativas internacionales reconocidas para el diseño e implementación de planes estratégicos en materia de seguridad de la información.

[4] https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa

[5] https://normas.gba.gob.ar/ar-b/decreto/2021/8/225112

[6] https://www.scba.gov.ar/subinformacion/Res1649_Plan_Integral_de_seguridad_SCBA.pdf

En resumen, se observa un camino claro y estandarizado que seguir a la hora de desarrollar planes, estrategias, normas, protocolos y medidas de ciberseguridad en organismos del estado y en el ambiente privado. Asimismo, la implementación de medidas de seguridad no puede concebirse como un modelo rígido, sino como un proceso dinámico, en el que las estrategias deben evolucionar conforme a los riesgos identificados y a las necesidades operativas del entorno donde se despliegan.

3 Situación Actual

En el inicio de la pandemia, la infraestructura tecnológica de la Suprema Corte de Justicia de la Provincia de Buenos Aires sufrió un evento de seguridad, el cual introdujo software malicioso. Este tipo de evento de seguridad, diseñado para explotar recursos computacionales, representó una grave amenaza para la estabilidad y seguridad de la tecnología e información allí almacenada.

Ante la detección del incidente, el Subsecretario de Tecnología Informática instruyó a todas sus áreas dependientes para actuar en conjunto en la contención y mitigación de la infección. Las acciones implementadas incluyeron: 1- Identificación y aislamiento de los equipos comprometidos, evitando la propagación del malware, 2- Desactivación de procesos sospechosos en los sistemas afectados y 3- Actualización y refuerzo de las medidas de seguridad, incluyendo parches de software y revisiones de configuración.

Una vez controlada la situación, se llevó a cabo un análisis exhaustivo para determinar el alcance del compromiso sufrido por la infraestructura, los activos afectados y la posible persistencia de código malicioso en los sistemas, y las vulnerabilidades explotadas para el ingreso del software malicioso.

Como resultado de esta evaluación, se decidió aplicar una medida de seguridad compleja pero efectiva: la migración de la infraestructura a nuevas máquinas virtuales. Además, se puso en evidencia la importancia de contar con protocolos sólidos de detección y respuesta a incidentes.

Las nuevas estrategias de seguridad preventiva aplicadas fueron: 1- Mayor monitoreo y análisis de la actividad en los activos informáticos, 2- Fortalecimiento de políticas de seguridad, reduciendo la posibilidad de compromisos futuros, 3- Despliegue de herramientas avanzadas de detección de amenazas, como soluciones de *Endpoint Detection and Response* (EDR), software antivirus basados en firmas, software específico de seguridad y análisis de vulnerabilidades y 4- Desarrollo de un Plan Integral de Seguridad de la Información.

4 Acciones en el marco del Plan Integral de Seguridad de la Información

Como resultado de los estudios realizados en materia de seguridad informática, surge la iniciativa de desarrollar un Plan Integral de Seguridad de la Información para la Suprema Corte de Justicia de la Provincia de Buenos Aires. Dicho plan se diseñó conforme a los lineamientos de la norma ISO/IEC 27001:2022, con el objetivo de establecer una

estrategia sólida y progresiva para la protección de los activos informáticos del organismo.

Desde el inicio del desarrollo del plan, se tomó una decisión estratégica clave: presentarlo en una versión reducida para su aprobación por parte de los ministros de la Suprema Corte. Esta estrategia se fundamentó en la premisa de que un plan integral completo podría no haber obtenido la aprobación requerida. El concepto de "plan reducido" hace referencia a un documento que contiene la estructura esencial de la norma, permitiendo que, mediante anexos y resoluciones posteriores, se incorporen gradualmente nuevas políticas de seguridad.

Para ejecutar el plan se definen una serie de acciones específicas implementadas en relación con las estrategias definidas en la sección anterior. La Tabla 1 permite visualizar de manera estructurada cómo cada estrategia se vincula con acciones concretas.

4.1 Objetivos de seguridad del plan y políticas implementadas

El Plan Integral de Seguridad de la Información fue aprobado mediante la Resolución N.º 1649 del año 2021, estableciendo los principales objetivos de seguridad:

- Identificación y análisis de riesgos informáticos que no se encuentran debidamente documentados dentro de los activos tecnológicos de la Suprema Corte de Justicia.
- Elaboración de un marco normativo que defina las pautas necesarias para la implementación de un modelo de Política de Seguridad de la Información, alineado con los riesgos identificados.
- Desarrollo e implementación de protocolos de seguridad, permitiendo al Área de Seguridad y Auditoría de la Suprema Corte ejecutar controles efectivos sobre los riesgos informáticos detectados.
- Aseguramiento del cumplimiento normativo, en consonancia con los lineamientos de la Subsecretaría de Tecnología Informática, así como con regulaciones y estándares provinciales, nacionales e internacionales.
- Aplicación transversal de la política de seguridad a todos los activos informáticos, tanto actuales como futuros, bajo la jurisdicción de la Suprema Corte de Justicia.

Entre las políticas implementadas en el marco del plan se encuentran la generación de contraseñas seguras y robustas y el respaldo de la información fuera de línea.

En relación a la política de contraseñas, se diseñó en función de los diferentes perfiles de usuario dentro de la infraestructura del Poder Judicial: 1- los usuarios básicos deben emplear contraseñas robustas, con una longitud mínima, requisitos de complejidad que incluyan mayúsculas, minúsculas y números y renovación periódica, sin reutilizar las últimas tres contraseñas y 2- los usuarios con permisos elevados, por la naturaleza crítica de su acceso, deben poseer contraseñas considerablemente más seguras, con una longitud mayor y cambios obligatorios en intervalos de tiempo más reducidos.

La política de respaldo de información se estableció con la modalidad fuera de línea, como una medida preventiva ante ataques de ransomware[7]. Se definió la ejecución de copias de seguridad de las bases de datos pertenecientes a cada uno de los departamentos judiciales, almacenándose en medios fuera de línea. De esta forma, se garantiza que, en caso de un ataque, se disponga de una copia de la información intacta y recuperable, evitando la encriptación simultánea de los datos de producción y sus respaldos.

Tabla 1. Relaciones entre Estrategias (primera columna) y Acciones (primera fila)

	Mayor monitoreo y análisis de la actividad en los activos informáticos	*Fortalecimiento de políticas de seguridad, reduciendo la posibilidad de compromisos futuros*	*Despliegue de herramientas avanzadas*	*Desarrollo de un Plan Integral de Seguridad de la Información*
Antivirus basado en firmas	☑		☑	
Antivirus de próxima generación	☑		☑	
Plan Integral de Seguridad de la información		☑		☑
Sandbox	☑		☑	
Análisis de vulnerabilidades	☑			
Servidores proxy para antivirus	☑		☑	
Capacitación constante de las delegaciones de tecnologia informática	☑	☑		
Boletín semanal de seguridad	☑			
Auditorías mediante bases de datos				☑

Además, conforma parte del plan, incluir aspectos de auditorías sobre las acciones realizadas en los distintos sistemas de información que integran la infraestructura tecnológica de la Suprema Corte de Justicia de la Provincia de Buenos Aires (SCBA). Estas auditorías son solicitadas tanto por los magistrados como por los agentes Subsecretaría de Control Disciplinario, asistiendo en la investigación los procesos disciplinarios. Cada solicitud de auditoría sigue un protocolo estructurado, asegurando la precisión y confiabilidad de los informes generados.

4.2 Antivirus basado en firmas para los puestos de trabajo

Se seleccionó la herramienta ESET[8], que fue desplegada exclusivamente en los puestos de trabajo, dejando fuera de su alcance a los servidores.

La elección de ESET estuvo fundamentada en la viabilidad económica y su facilidad de implementación y mantenimiento - ESET podía desplegarse de forma masiva y rápida, sin necesidad de un período de ajuste ni impacto en la operatividad-.

[7] En este contexto se entiende por software malicioso que en primer lugar encripta los datos de la víctima y luego demanda un pago para obtener la llave para desencriptar.

[8] https://www.eset.com/ar/

Esta elección estratégica permitió una protección efectiva y centralizada en los puestos de trabajo, minimizando la exposición a amenazas comunes, la reducción de la carga operativa del equipo de seguridad, al tratarse de una herramienta con una gestión simple y automatizada y el despliegue rápido y eficiente, sin afectar el rendimiento de la infraestructura ni requerir configuraciones complejas.

Dada la infraestructura de comunicación heterogénea que caracteriza a la Suprema Corte de Justicia de la Provincia de Buenos Aires, se identificó la necesidad de implementar soluciones que optimicen el uso de los recursos de conectividad, especialmente en aquellas localidades donde el servicio de internet es limitado o inestable.

El principal inconveniente detectado estaba relacionado con la actualización del sistema de protección antivirus ESET, cuya arquitectura requería que cada equipo realizará una conexión al centro de datos ubicado en la ciudad de La Plata (Provincia de Buenos Aires, Argentina) para solicitar el paquete de actualización correspondiente. Este proceso, al estar centralizado, provocaba saturación en la conectividad del centro de datos y afectando el rendimiento de otros servicios críticos.

Para mitigar este impacto, se implementó un esquema de servidores proxy locales en cada una de las delegaciones de tecnología informática. Su despliegue departamental minimizó la cantidad de saltos de red y la latencia en la comunicación. Adicionalmente, se permitió la instalación de estos servidores en puntos con mala conectividad.

4.3 Antivirus de próxima generación

Con el objetivo de fortalecer la seguridad de los sistemas críticos de la Suprema Corte de Justicia de la Provincia de Buenos Aires, se adoptó una solución avanzada de *Endpoint Detection and Response* (EDR) de la firma Fortinet[9]. Esta tecnología, basada en *machine learning*, permite una detección y respuesta proactiva ante amenazas emergentes.

Dado que el ecosistema del centro de datos cuenta con aplicaciones, protocolos y flujos de comunicación altamente especializados, fue necesario llevar a cabo un entrenamiento previo del sistema para garantizar una detección precisa de anomalías y posibles amenazas. Este proceso incluyó: 1- Análisis del tráfico de red y protocolos utilizados dentro de la infraestructura, 2- Evaluación del comportamiento de las aplicaciones críticas, con el fin de evitar falsas alertas y 3- Monitoreo de patrones de uso para establecer una base de referencia confiable.

Para minimizar riesgos y evitar bloqueos inesperados de procesos esenciales, la herramienta se implementó inicialmente a modo de simulación. Durante un período de 90 días, se realizaron análisis detallados de procesos, comportamientos y comunicaciones, permitiendo ajustar los parámetros de detección y respuesta.

Tras la fase de evaluación y optimización, el sistema EDR fue activado en modo de protección activa, proporcionando una protección avanzada y automatizada ante posibles ataques. Entre los principales beneficios de esta implementación se destacan: 1- Mayor precisión en la detección de amenazas, gracias al aprendizaje previo de la infraestructura y comunicaciones, 2- Reducción de falsos positivos, evitando interrupciones en sistemas esenciales, 3- Capacidad de respuesta automatizada, permitiendo contener

[9] https://fortinet.all-kom.com/index.html#main

incidentes en tiempo real y 4- Adaptabilidad a nuevas amenazas, mediante la actualización continua de modelos de *machine learning*.

4.4 Sandbox

Con el objetivo de fortalecer la seguridad de la infraestructura informática, se procedió a la adquisición e implementación de una solución tipo *sandbox*. Esta herramienta fue diseñada para integrarse con los *firewalls* existentes, los servidores de correo y el sistema de protección EDR, permitiendo la detección y análisis avanzado de amenazas en un entorno controlado.

Uno de los principales retos en la implementación fue la integración con el sistema de protección EDR, ya que dicho sistema opera dentro de una nube privada del proveedor, lo que imposibilitaba una conexión directa desde la infraestructura interna.

Para resolver este inconveniente se implementó una máquina virtual como punto de canalización, mediante la cual se gestionaría todo el tráfico de conexión hacia el sistema EDR, exponiendo únicamente una dirección IP y un puerto específico.

Esta solución actúa como puente seguro entre la infraestructura *on-premise*[10] y las aplicaciones de terceros, centralizando la comunicación y reduciendo significativamente la superficie de ataque.

Gracias a esta implementación, se logró una integración efectiva entre el *sandbox* y el sistema EDR, combinando sus capacidades de detección y análisis en un entorno unificado. De este modo, ambas herramientas, que de manera independiente ya aportan un alto nivel de seguridad, ahora operan en conjunto, proporcionando una protección aún más robusta y eficiente contra amenazas avanzadas.

4.5 Análisis de vulnerabilidades

Con el propósito de identificar brechas de seguridad y posibles vulnerabilidades en los sistemas informáticos de la Suprema Corte de Justicia de la Provincia de Buenos Aires, se llevó a cabo un análisis exhaustivo utilizando software libre sobre una distribución de Linux[11] especializada en seguridad informática. Para ello, se emplearon diversas herramientas diseñadas para la detección y evaluación de riesgos en los activos digitales.

El análisis se realizó mediante la ejecución de *scripts* de evaluación de seguridad, con el objetivo de detectar puntos débiles sin afectar la disponibilidad ni el correcto funcionamiento de los sistemas. Entre las herramientas utilizadas se destacan: DNSRecon[12], Sublist3r[13], OWASP[14] y NMAP[15](con los distintos parámetros aplicables para cada tipo de análisis).

---

[10] Infraestructura (servidores, enlaces, sistemas de almacenamiento y otros componentes tecnológicos) que se encuentra ubicada en las instalaciones de la organización.

[11] Sistema operativo open source. https://www.linux.org/

[12] https://www.kali.org/tools/dnsrecon/

[13] https://www.kali.org/tools/sublist3r/

[14] https://owasp.org/

[15] https://nmap.org/

4.6 Capacitación constante de las delegaciones de tecnología informática

Dado el alto volumen de equipos a controlar y la diversidad de infraestructura distribuida en los distintos departamentos judiciales, se tomó la decisión estratégica de transferir la ejecución de ciertas tareas operativas a las Delegaciones de Tecnología Informática. Esta migración permitió una administración más eficiente y descentralizada, asegurando que cada delegación tuviera autonomía operativa.

Para garantizar una transición ordenada y segura, se implementaron las siguientes acciones: 1- Asignación de usuarios con permisos de solo lectura en las consolas de administración de los productos de seguridad, evitando alteraciones no autorizadas en la configuración de los sistemas y 2- Implementación de un programa de capacitación continua, con el objetivo de instruir al personal técnico de cada delegación en el uso y mantenimiento de las herramientas de seguridad.

4.7 Boletín semanal de seguridad

Dado el volumen creciente de información generada por los sistemas de protección y detección de amenazas, así como la limitada disponibilidad de personal técnico para atender estos sistemas, se identificó la necesidad de crear un mecanismo eficiente de comunicación y acción. Este mecanismo debía permitir que los técnicos del interior de la provincia de Buenos Aires recibieran únicamente la información relevante, junto con las acciones recomendadas para su resolución.

Para garantizar la efectividad de los boletines de seguridad, se definió qué tipo de información sería compartida con las delegaciones de Tecnología Informática. Inicialmente, el boletín incluyó: 1- Amenazas detectadas en las consolas de seguridad, 2- Estado de protección de los dispositivos (desactualizados o desconectados) y 3- Detección de instalación de software no permitido y otras alertas críticas.

5 Conclusiones y Trabajos Futuros

Este trabajo permitió identificar una serie de problemáticas relacionadas con la ciberseguridad dentro de la infraestructura tecnológica de la Suprema Corte de Justicia de la Provincia de Buenos Aires (SCBA). Como respuesta a estas vulnerabilidades, el personal del Área de Seguridad y Auditoría desarrolló diversas acciones estratégicas que generaron efectos positivos de manera transversal, alcanzando a todas las áreas que integran la Subsecretaría de Tecnología Informática y sus respectivas Delegaciones de Tecnología Informática (DTI).

Asimismo, resulta fundamental resaltar la relevancia y necesidad que impulsó el desarrollo del Plan Integral de Seguridad de la Información, mediante el cual se llevó a cabo un análisis exhaustivo y detallado de los activos tecnológicos, los procesos involucrados y los tiempos operativos específicos del ámbito de la justicia provincial.

En este contexto, fue clave la utilización de conceptos establecidos en las estrategias nacionales y provinciales vigentes, así como también la integración de los aportes realizados por (D'Agostino et al., 2021). La Suprema Corte de Justicia de la Provincia de Buenos Aires desarrolla sus actividades en un contexto provincial que cuenta con una

normativa propia en materia de seguridad informática, la cual, a su vez, está integrada en el marco más amplio de la legislación nacional de la República Argentina. Por esta razón, resultó fundamental que las políticas y acciones llevadas a cabo por la SCBA se alinearan adecuadamente con las regulaciones provinciales y nacionales, con el propósito de generar una armonización efectiva en el funcionamiento entre los distintos niveles gubernamentales (Nacional, Provincial y SCBA).

Se debe destacar que, en cada uno de los despliegues y desarrollos mencionados en la Sección 4 fue imprescindible contar con la predisposición, compromiso y colaboración activa de las distintas áreas involucradas, tales como el Área de Comunicaciones, el Área de Infraestructura y Bases de Datos, el Área de Desarrollo y el Área de Asistencia al Usuario, cuya participación fue decisiva para alcanzar los objetivos propuestos.

Cabe resaltar también, la necesidad de contar con un mayor número de profesionales especializados en ciberseguridad, tanto desde la perspectiva defensiva como ofensiva. El contexto actual requiere de profesionales debidamente capacitados que sean capaces de afrontar con solvencia los desafíos relacionados con la protección de la información y los activos tecnológicos. Esta necesidad se ve potenciada por la constante evolución y creciente dependencia de la tecnología en distintos ámbitos, así como por la implementación continua de sistemas informáticos orientados a mejorar la calidad de vida de los ciudadanos desde la administración pública. Por ello, resulta esencial fomentar la formación y especialización de profesionales en esta área, para asegurar una adecuada protección de los activos digitales y fortalecer la capacidad de respuesta ante amenazas emergentes.

5.1 Trabajos futuros

Entre los trabajos futuros se encuentra la implementación de una normativa específica que regule claramente el uso adecuado de los activos informáticos. Dicha normativa debería contemplar el correcto uso de computadoras, servicios en red (como carpetas compartidas y almacenamiento en la nube), telefonía móvil, así como los activos tecnológicos en general y, especialmente, el uso responsable de internet y el correo electrónico.

Otro proyecto pendiente de desarrollo es la política de respaldos inmutables, cuya principal característica consiste en aislar copias de seguridad de manera que éstas no puedan ser modificadas bajo ningún concepto. La implementación de esta política permitirá aumentar sustancialmente el grado de protección de la información, incluso frente a incidentes críticos como ataques de *ransomware*.

Asimismo, es indispensable contar con protocolos claros y precisos que permitan a cualquier usuario, independientemente de su nivel de formación técnica, llevar adelante con eficacia las tareas asignadas. En este sentido, es particularmente relevante la implementación de un protocolo de respuesta ante amenazas, que contemple un procedimiento detallado y secuencial, indicando las acciones que deben ejecutar cada uno de los actores involucrados para lograr la rápida subsanación del incidente malicioso.

Finalmente, es prioritario destacar la necesidad imperiosa de elaborar un plan integral de recuperación ante desastres. Este plan permitirá definir con claridad los protocolos y acciones necesarias para restaurar, en el menor tiempo posible, todos los servicios que ofrece la SCBA ante incidentes graves que comprometan su operatividad.

Cabe aclarar que, la ejecución de estos proyectos no requiere necesariamente la adquisición de herramientas comerciales o propietarias, sino que también puede realizarse a través del empleo de software libre, cuya disponibilidad y calidad son ampliamente reconocidas, o bien, mediante el desarrollo de soluciones propias dentro del organismo.

Es imprescindible destacar la necesidad de mantener un proceso constante de formación y concientización en materia de ciberseguridad. Una capacitación continua en esta área resulta fundamental para sostener un nivel adecuado de protección ante la permanente evolución de las amenazas que emergen diariamente a nivel global. De esta manera, se contribuye a mantener una postura preventiva y proactiva frente a incidentes potenciales, asegurando así la resiliencia y seguridad de la información en el tiempo. En virtud de lo expuesto, resulta fundamental desarrollar e implementar un plan de capacitación destinado a los usuarios, el cual debe realizarse de forma periódica y poseer un carácter obligatorio. La capacitación en materia de ciberseguridad constituye una herramienta esencial para asegurar un uso responsable y seguro de los recursos tecnológicos que intervienen constantemente en nuestra vida diaria. A través de estas acciones educativas se busca fortalecer la conciencia sobre los riesgos y buenas prácticas en el manejo de las tecnologías, contribuyendo así al incremento general de la seguridad informática institucional y personal.

Referencias

D'Agostino, S., Steinmetz, A., & Kruse, D. (2021). Estrategia de ciberseguridad 2021-2024 de la provincia de Buenos Aires. In *XV Simposio de Informática en el Estado (SIE 2021)-JAIIO 50 (Modalidad virtual)*. ISSN: 2451-7534 - Página 260-271

Decreto 8/2021. Provincia de Buenos Aires. Argentina (https://normas.gba.gob.ar/ar-b/decreto/2021/8/225112)

Furstenau, L. B., Sott, M. K., Homrich, A. J. O., Kipper, L. M., Al Abri, A. A., Cardoso, T. F., ... & Cobo, M. J. (2020, March). 20 years of scientific evolution of cyber security: A science mapping. In International conference on industrial engineering and operations management (pp. 314-325). IEOM Society International.

International Telecommunication Union. (2009). Overview of cybersecurity. ITU-T Recommendation X.1205.

MAGERIT 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (2012). https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Plan Integral de Ciberseguridad de la Provincia de Buenos Aires (2021). https://normas.gba.gob.ar/documentos/xpzbRYH3.html

Resolución 44/2023. Secretaría de Innovación Pública. Jefatura de Gabinete de Ministros. República Argentina (https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-44-2023-389245/texto

Warner, M. (2012). Cybersecurity: A pre-history. Intelligence and National Security, 27(5), 781-799.